UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/818,914 | 03/26/2001 | W. Dale Hopkins | 20206-16 (P00-3324) | 4267 |

22879 7590 09/07/2005

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

| EXAMINER | |
|---|---|
| CALLAHAN, PAUL E | |
| **ART UNIT** | **PAPER NUMBER** |
| 2137 | |

DATE MAILED: 09/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/818,914 | HOPKINS ET AL. | |
| | Examiner | Art Unit | |
| | Paul Callahan | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *13 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-63* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34 and 36-63* is/are rejected.

7)☐ Claim(s) *35* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) ~~Paper No(s)/Mail Date~~ _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

### *Response to Amendment*

1. Claims 1-63 are pending in this application and have been examined.

### *Response to Arguments*

2. The applicant argues in traverse of the rejection of the claims as obvious over Menezes in view of Quisquater by asserting that the claims may be distinguished from the applied prior art since "Candidates are selected and tested one candidate at a time in a sequential manner." The applicant asserts that this is distinguished from the claim language where a plurality of candidates are selected and then tested. The Examiner counters that Menezes teaches a search strategy that begins with an interval of odd numbers generated randomly, and then tests the numbers over the interval for primality. his does indeed read on the claim limitations of generation of a plurality of random odd numbers and subsequent testing for primality.

The applicant argues that the Quisquater reference does not teach performing exponentiation operations in parallel. Yet such is indeed taught by the reference at the sections indicated in the rejection of the claims where Quisquater discusses exponentiation in parallel at the section cited in the rejection of the claims.

The applicant asserts that the previous Office Action failed to make a prima facie case for obviousness over the applied prior art because: "The Examiner appears to make no assertion that these features are present in Quisquater..." Yet a careful reading of the previous Office Action in the case reveals that such a showing of prior art was indeed made on page 3 in the third subparagraph of paragraph five where the

Examiner wrote: "However Quisquater et al. teaches such a parallel arrangement of exponentiators (fig. 1, page 2 paragraph 7)..."

The applicant asserts that there was no proper statement of a motive to combine the teachings of Menezes and Quisquater. Yet a careful reading of the Office Action reveals that such a statement was made where the Examiner pointed to Section 4.1 of Menezes which discusses the advantages of rapid exponentiation parallel processing in the generation of RSA keys, something that would certainly be provided by the system of Quisquater.

The applicant asserts that the search intervals of Menezes cannot be considered as random. Yet a careful reading of Menezes reveals that they are based on a random seed value and therefore can be consider as random sequences.

The applicant asserts that the Quisquater reference does not represent analogous art the instant invention. Yet the Quisquater reference is directed towards the rapid generation of RSA keys, as is the applicant's invention according to his own "Background of the Invention" section of his specification.

The applicant asserts that the term "substantially simultaneously" is definite and well defined by the specification. The Examiner counters by noting that the term is self-contradictory, events either happen simultaneously or they don't, mere overlap in time does not convert such events into simultaneous events.

**Claim Rejections - 35 USC § 112**

3. The following is a quotation of the second paragraph of 35 USC 112:

*The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.*

4. Claims 5-11, 15-27, 30, 39-41, 47, 53, and 58-62 are rejected under 35 USC 112 second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention. The claim contains the phrase: "substantially simultaneously" It is not clear what is meant by "substantially" in this context.

**Claim Rejections - 35 USC § 103**

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

*(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

6. Claims 1-7, 9-18, 20-34, and 36-63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Handbook of Applied Cryptography, Menezes et al., CRC Press 1996, pages 134-168, and Quisquater et al., "Fast Decipherment Algorithm for RSA Public Key Cryptosystem," Oct. 1982, Electronic Letters, Vol. 19, No. 21.

As for claims 1, 5, 6, 24, and 45, Menezes teaches a process of searching for a plurality of prime number values, comprising the steps of: randomly generating a

plurality of k random odd numbers each providing a prime number candidate (Sec. 4.1.1, p. 134); and performing a plurality of t primality tests on each of the plurality of k randomly generated prime number candidates (Sec. 4.1.1, p. 134), each of the plurality of (k x t) primality tests including an associated exponentiation operation (Sec. 4.2.3 p. 138-140). Menezes does not teach a processing system including a processing unit and a plurality (k x t) of exponentiation units communicatively coupled to the processing unit, or that the primality tests are carried out by the plurality of exponentiation units in parallel and where the exponentiation operations are carried out substantially simultaneously. However Quisquater et al, teaches such a parallel arrangement of exponentiators (fig. 1, page 2 paragraph 7). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the method of Menezes. It would have been desirable to do so as this would allow for computation to proceed more rapidly. The motivation to make this combination is found for example, in Menezes Sec. 4.1 Introduction where the efficiency of generation of public key parameters in public key systems such as RSA is discussed.

As for claim 3, Menezes teaches each of said plurality of prime number candidates has a specified length and wherein said plurality y of additional odd numbers defines an interval that is selected relative to said specified length (Sec. 4.1.1)

As for claim 13, Menezes teaches a step of performing at least one primality test that includes performing a Miller-Rabin type primality test (Sec. 4.2.3).

As for claim 14, Menezes teaches a step of randomly generating a plurality of k random odd numbers that further includes: defining a length L for each of the plurality of k random numbers to be generated; and generating each of said plurality of k random odd numbers in an interval between 2L and 2L-1 (Sec. 4.4.3).

As for claims 15, and 17, Menezes teaches a process of searching for a plurality of prime number values comprising the steps of: randomly generating at least one random odd number providing a prime number candidate (sec. 4.1.1); determining a plurality of y additional odd numbers based on said at least one randomly generated odd number to provide y additional prime number candidates (sec. 4.1.1), thereby providing a total number of y+1 candidates (sec. 4.1.1); performing at least one primality test on each of said y+1 candidates (sec. 4.2.3), each of the y+1 primality tests including an associated exponentiation operation (sec. 4.2.3.) Quisquater teaches the features not taught by Menezes, namely a plurality of exponentiation units communicatively coupled with a processing unit, executed by an associated one of the y+1 of the exponentiation units, said y+1 exponentiation operations being performed by said associated y+1 exponentiation units substantially simultaneously (fig. 1, page 2 paragraph 7). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the method of Menezes. It would have been desirable to do so as this would allow for computation to proceed more rapidly. The motivation to make this combination is found for example, in Menezes Sec. 4.1 Introduction where the efficiency of generation of public key parameters in public key systems such as RSA is discussed.

As for claims 2, 7, 9-11, 18, 20, 25, 27, 28, 30, and 46-49, Menezes teaches a prime number generating process of searching in parallel for a plurality of prime number values, comprising the steps of randomly generating a plurality of k random odd numbers expressed as no,o, nl,o, . n((k-1)),0, each said number providing a prime number candidate; determining a plurality of y additional odd numbers based on each one of the randomly generated odd numbers no,o, nl,o, n(k-1),O to provide (k X y) additional prime number candidates (no,,, 110,2, no,y), (nl,l, n1,2, n1,y), . (n(k-1),1, n(k-1),2, n(k-1);,) thereby yielding a total number of (k r (y+1)) prime number candidates (Page 148, Sec. 4.5.1); sieving said (k x (y+1)) prime number candidates by performing a small divisor test on each of said candidates in order to eliminate

candidates revealed to be composite numbers by said small divisor test thereby yielding a sieved number s of candidates (Page 145, Sec. 4.4.1); and performing at least one primality test on each of said sieved number s of candidates (Page 148, Sec. 4.5.1), each of the plurality of s primality tests including an associated exponentiation operation (Page 146, Sec 4.4.1). Menezes does not teach the exponentiation operations being executed by an associated one of a plurality of the exponentiation units, where the exponentiation operations are performed by a plurality of exponentiation units substantially simultaneously. However Quisquater does teach such an arrangement of parallel exponentiators, (fig. 1, page 2 paragraph 7). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the method of Menezes. It would have been desirable to do so as this would allow for computation to proceed more rapidly. The motivation to make this combination is found for example, in Menezes Sec. 4.1 Introduction where the efficiency of generation of public key parameters in public key systems such as RSA is discussed.

As for claims 4,16, 29, and 34, Menezes teaches a prime number generating system as recited in wherein said step of determining a plurality of y additional odd numbers based on each one of the randomly generated odd numbers no,o, nl,o, .. . n(k-1),O includes successively adding two to each of said randomly generated odd numbers no,o, nl,o, . n(k-1),O to provide (k x y) additional prime number candidates expressed as (no,1= no,o+ 2 , no,2 -=no,o+ 4, . no,y = lio,o + (y-2)), (nl,l = n1,o+ 2 , n1,2= n1,o+ 4, n1,y = nl,o + (y-2)), . (n(k_1),1= n~k-1)>o+ 2 , n(k-1),2=n'-k-1),o+ 4, n(k_1),y = n(k-1),O +(y.2)). (Page 148, Sec. 4.5.1).

As for claims 12, 21, 31, and 50, Menezes teaches a prime number generating system wherein said step of performing at least one primality test includes performing a Fermat type primality test. (Sec. 4.2.1).

As for claims 13, 22, 32, and 51, Menezes teaches a prime number generating system wherein said step of performing at least one primality test includes performing a Miller-Rabin type primality test. (Sec. 4.2.3).

As for claims 23, 33, and 52, Menezes teaches a prime number generating system wherein said step of randomly generating a plurality of k random odd numbers further includes: defining a length L for each of the plurality of k random numbers to be generated; and generating each of said plurality of k: random odd numbers in an interval between 2L and 2L_1. (Sec. 4.4.3).

As for claims 54-63, the claims represent the computer program product embodied in a memory medium which when read out, causes the system of Claim 1 to carry out the process of generating prime numbers, and therefore is rejected on the same basis as claim 1.

As for claims 36-44, and 53, the claims are directed to the apparatus carrying out the method of claims 1-14 and are therefore rejected on the same basis as are those claims

***Allowable Subject Matter***

7. Claim 35 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

**Conclusion**

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

9/1/05

Paul Callahan

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER